

WHAT IS CLAIMED IS:

1. A provisioning system that secures delivery of a client public key, the provisioning system comprising:
 - a client to be registered;
 - a provisioning server for registering the client and assigning it a unique user ID (identification);
 - a key distribution center for generating a provisioning key associated with the user ID, the provisioning key being forwarded to the provisioning server;
 - the provisioning server generating configuration parameters for initializing the client, the provisioning key being included in the configuration parameters; and
 - upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center.
2. The provisioning system of claim 1 wherein the key distribution center stores the public key or generates a certificate.
3. The provisioning system of claim 1 further comprising a provisioning ticket in which the provisioning key is also enclosed.
4. The provisioning system of claim 1 further comprising a provisioning ticket for forwarding the provisioning key to the client.
5. The provisioning system of claim 4 further comprising a ticket granting ticket obtained with an AS Request that is authenticated using a public key previously registered with the provisioning ticket, the ticket granting ticket used by the client for obtaining further tickets from the KDC, where each further ticket is used for obtaining access to a particular server.
6. The provisioning system of claim 1 wherein the client further provides to the provisioning system a host identifier that uniquely identifies a computer on which the client application is running.
7. A method for initially establishing trust between a KDC (Key Distribution Center) and a client having a uniquely identifiable user ID (identification) that was assigned by the provisioning server, the method comprising:

generating, by the KDC, a provisioning key associated with the user ID, the provisioning key being forwarded to the provisioning server;

forwarding the provisioning key to a provisioning server for registering the client;

generating, by the provisioning server, configuration parameters for initializing the client;

forwarding to the client, the provisioning key and the configuration parameters for initializing the client; and

upon initialization, the client provides its public key, authenticated with the provisioning key for forwarding to the key distribution center.

8. The method of claim 7 further comprising
a provisioning ticket for forwarding the provisioning key to the client.

9. The method of claim 8 further comprising
a ticket granting ticket obtained with an AS Request that is authenticated using a public key previously registered with the provisioning ticket, the ticket granting ticket used by the client for obtaining further tickets from the KDC, where each further ticket is used for obtaining access to a particular server.

0996657 092601
T09260" 25599660